ILLUSTRATIVE SAMPLE · SYNTHETIC TARGET & FIGURES

STRICTLY PRIVATE & CONFIDENTIAL · PREPARED FOR THE INVESTMENT COMMITTEE

TECHNOLOGY DUE DILIGENCE — IC REPORT

Project Cobalt

«Codename» · report date «illustrative» · run «illustrative» · target name withheld by design

CONDITIONAL-GO

Acquire and integrate a multi-tenant B2B SaaS platform — subject to **three conditions cleared before close**. The model's aggregate risk picture would read GO; the deal mandate, enforced in code, clamps it.

Clamp: one critical security gate is failing (SOC 2 Type II incomplete) and one critical diligence question is unanswered (production DR untested). The reason is shown, never buried.

6.5
MANDATE FIT /10

DD Prepared by DD Memo · AI-native Technology Diligence Service

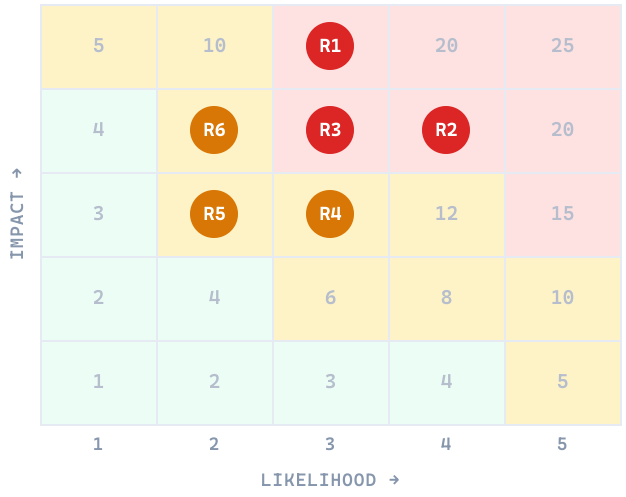
1 · Executive summary

The evidence supports acquisition subject to three conditions being cleared before close. Northwind is a credible multi-tenant B2B SaaS platform whose architecture and engineering culture are broadly fit for purpose, but three red flags gate the deal until resolved: an **untested disaster-recovery posture** against a 99.9% SLA, an **incomplete SOC 2 Type II**, and **two unremediated critical/high penetration-test findings**. None is an absolute deal-breaker; all three are clearable conditions. On a triangulated basis, two management headline figures — 99.9% uptime and ~40% test coverage — did not survive independent re-derivation (~99.72% and ~28% respectively) and are flagged for management response.

3	2	$1.8M	$1.1M	16
RED FLAGS	FAILING CRITERIA	YEAR-1 CASH	RUN-RATE SYNERGY / YR	EVIDENCE REVIEWED

Findings at a glance

REF	DOMAIN	STATUS	RED	YELLOW	OPEN
D1	Architecture & Scalability	Critical	1	1	1
D2	Security & Resilience	Critical	2	1	·
D3	Privacy & Data Governance	Caution	·	1	1
D4	Third-Party & Vendors	Caution	·	1	·
D5	Engineering & Key-Person	Caution	·	2	1
D6	Operations & SRE	Caution	·	1	·
D7	Integration / General	Clear	·	·	·



Open red/amber risks on the 5×5 likelihood × impact matrix; R1–R3 (red) sit in the critical band, R4–R6 (amber) in the moderate band. Cell numbers show the L×I score.

2 · Key risks & deal-breakers

2 FAILING **Constitutional violations**

SOC 2 Type II must be complete at close (enterprise-renewal gate). · observed: in progress `MANDATE-SEC-02`

Production DR must be tested against the contractual SLA before close. · observed: no failover exercise in 12 months `MANDATE-ARCH-01`

No absolute deal-breakers identified. Open red flags are repriceable or addressable as conditions of a Conditional-Go.

Red flags (3)

The platform runs single-region; DR is undocumented and untested — the 99.9% SLA is unproven.

Require a tested DR runbook with dated failover evidence (RTO/RPO) as a condition of close. Triangulation of the 12-month incident log yields ~99.72% availability vs. the ≤8.8h/yr the SLA implies.

Evidence: `ARCH-DIAG-01` `OPS-INC-LOG`

ARCHITECTURE
CRITICAL
L3 × I5
$650,000

SOC 2 Type II is incomplete and ISO 27001 has not started — blocks enterprise renewals.

Obtain a written SOC 2 completion date, or a price/escrow adjustment for the compliance gap. Two enterprise renewals named in the CRM export already gate on it.

Evidence: `SEC-CERT-STATUS`

SECURITY
CRITICAL
L4 × I4
$180,000

Two critical/high penetration-test findings remain unremediated past SLA.

Require a written remediation commitment and timeline before close. ⚔ **Verified:** management's questionnaire claimed "no open criticals"; an independent pass re-read SEC-PEN-02, found two past-SLA items, and **downgraded the claim** rather than presenting it as fact.

Evidence: `SEC-PEN-02`

SECURITY
CRITICAL
L3 × I4
$120,000

Yellow flags (3)

Bus factor of 2 on the billing/entitlements core; contractor IP assignment is unevidenced.

90-day post-close cross-training plan; collect signed IP-assignment agreements for the three unlisted git contributors. ◈ **Triangulated:** stated "~40% coverage" re-derives to ~28% on core services from CI artifacts.

Evidence: `ENG-ORG` `ENG-IP` `ENG-CI-01`

ENGINEERING
MODERATE
L3 × I3
$30,000

EU customer data flows to a US data-enrichment vendor without a documented transfer mechanism.

Complete the RoPA; put SCCs / a transfer-impact assessment in place as a post-close remediation.

PRIVACY

MODERATE

L2 × I3

Evidence: `PRIV-ROPA` `VEND-03`

Three vendors are single points of failure; the payments contract has no change-of-control clause.

Renegotiate change-of-control consent and substitutability at integration. Identity, payments and enrichment are each un-substitutable on <90 days' notice.

VENDORS

MODERATE

L2 × I4

Evidence: `VEND-01` `VEND-02` `VEND-03`

3 · Deal thesis & valuation impact

Deal thesis after diligence

Northwind remains an attractive bolt-on: a modern multi-tenant platform whose identity stack overlaps the acquirer's, converting a diligence risk into a consolidation synergy. The thesis holds provided the three conditions are cleared; diligence surfaces no structural reason to walk.

Valuation impact

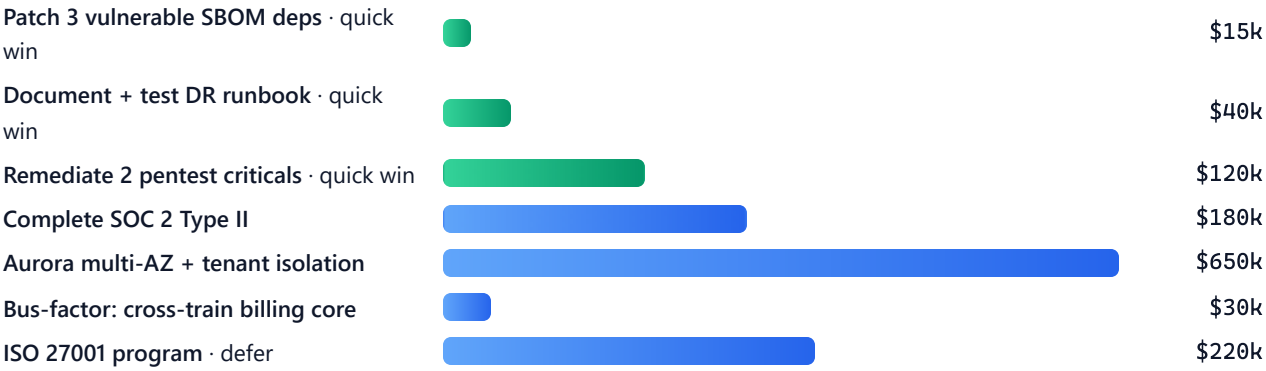
The ~$1.8M remediation envelope and the compliance gap argue for a modest price adjustment or escrow rather than a re-rate. The two overstated management metrics (uptime, coverage) marginally soften the operational-quality story but do not move the base-case valuation; the DR and SOC 2 conditions are the live levers on price.

Synergies

Identity and observability consolidation onto the acquirer's standard stack, plus avoided compliance duplication, net ~$1.1M/yr run-rate at steady state — half-ramped in year one, mapped to the acquirer's own integration playbook.

4 · Integration economics

OTE (one-time)	CAPEX	Year-1 cash impact	Synergy / yr
$1,150,000	$650,000	$1,800,000	$1,100,000



Remediation & integration line items, impact-ranked; green bars are the low-effort quick wins that clear two of the three close conditions. Total illustrative envelope ~$1.8M over 18 months.

Cost to close. The three quick wins — patch the SBOM dependencies, test the DR runbook, remediate the two pentest criticals (~$175k combined) — clear two of the three close conditions and should be pre-agreed in the SPA.

Year-1 program. SOC 2 completion and the Aurora multi-AZ / tenant-isolation project are the two major year-one workstreams (~$830k together).

Run-rate economics. Net run-rate value reaches +$1.1M/yr once identity consolidation lands; the high-cost sensitivity case requires that consolidation in year one.

Key assumptions the IC must accept:

- Identity consolidation completes within year one.
- Synergy realization lands within ±30% of plan.
- No additional criticals surface during SOC 2 completion.

Alternatives & trade-offs. Deferring ISO 27001 (the thankless quadrant) preserves ~$220k with no near-term revenue impact — recommended.

5 · Conditions & SPA implications

Conditions of a Conditional-Go

1. Written remediation commitment + timeline for the two open critical/high pentest findings.
2. SOC 2 Type II completion date in writing, or a price/escrow adjustment for the compliance gap.
3. A **tested** disaster-recovery runbook evidencing the contractual 99.9% SLA.

SPA implications

The three conditions map to closing conditions and a compliance escrow; the vendor change-of-control gap argues for a specific indemnity. Counsel should treat the DR and SOC 2 items as conditions precedent, not post-close covenants.

Deal structuring

Open findings rolled into negotiation mechanics — a certain price adjustment, milestone-released escrow, and the reps & warranties to require. Deterministic from the risk register (§2).

LEVER	AMOUNT
Price adjustment — certain remediation to clear the red conditions	−$340,000
Escrow / holdback — milestone-released	$500,000

Escrow releases: $150k on a tested DR runbook · $200k on SOC 2 Type II completion in writing · $150k on the pentest remediation plan.

Reps & warranties to require: Security — no undisclosed incidents; Privacy — GDPR + a lawful EU→US transfer mechanism; Engineering — all contributor IP assigned; Vendors — payments MSA assignable at change of control.

Retention: founder / key-engineer lockup + knowledge-transfer on the billing core (bus factor of 2). **Earnout:** tie deferred consideration to year-1 run-rate synergy ($0.6M).

Draft SPA provisions

Auto-drafted from the open risk register for counsel to mark up — closing conditions and escrows gate the deal; indemnities and warranties reprice or disclose.

CLOSING CONDITION — RED

SOC 2 Type II incomplete

Gates two named enterprise renewals; a compliance gap that reprices the deal.

> "Completion of SOC 2 Type II certification (or an agreed compliance escrow) shall be a condition precedent to Closing."

ESCROW — YELLOW · $180,000

Compliance & remediation escrow

Holds back consideration against SOC 2 completion and pentest remediation.

> "$180,000 of the consideration shall be held in escrow for 12 months against completion of SOC 2 Type II and remediation of the two open penetration-test findings."

INDEMNITY YELLOW

Vendor change-of-control exposure

The payments MSA is silent on assignment at change of control — a live integration risk.

> "Seller shall indemnify Buyer for costs arising from the absence of change-of-control consent in the payments master services agreement."

6 · Outstanding diligence items

- DR test evidence — a runbook with a dated failover exercise (RTO/RPO). (Clears Condition 3.)
- Completed RoPA + the SCC / transfer-impact assessment for the US enrichment flow.
- Signed IP-assignment agreements for the three unlisted git contributors.
- Written status and remediation timeline for the two open pentest criticals. (Clears Condition 1.)

7 · Scope limitations & evidence requested

This assessment is limited by the evidence made available. The findings and recommendation above should be read with these caveats:

- LIMITATION No DR test evidence was available; the SLA could not be independently confirmed and was re-derived from the incident log.
- LIMITATION The RoPA is incomplete; cross-border transfer exposure is estimated, not confirmed.
- LIMITATION Uptime and test-coverage figures are re-derived from artifacts, not audited.

Documents requested from the seller

Providing these artifacts and re-running diligence would upgrade this to a full-scope assessment:

- A DR runbook with a dated failover exercise (RTO/RPO).
- Records of processing + the SCC/TIA for the US enrichment flow.
- Signed IP-assignment agreements for the three unlisted contributors.
- The two open penetration-test findings and their remediation status.

Appendix · Findings & evidence

Per-workstream findings

RED Single-region platform; DR undocumented and untested vs. a 99.9% SLA. arch-agent · high conf ARCH-DIAG-01 OPS-INC-LOG

YELLOW Aurora runs a single writer under multi-tenant load — a scaling ceiling and noisy-neighbour risk. arch-agent · med conf ARCH-DIAG-01

RED SOC 2 Type II "in progress," not complete; ISO 27001 not started. security-agent · high conf SEC-CERT-STATUS

RED Last pentest left two critical/high findings unremediated past SLA. security-agent · high conf SEC-PEN-02

YELLOW SBOM shows three known-vulnerable transitive dependencies in shipped services. security-agent · high conf SEC-SBOM-01

YELLOW EU customer data flows to a US enrichment vendor without a documented transfer mechanism. privacy-agent · med conf PRIV-ROPA VEND-03

YELLOW Three vendors are single points of failure; payments MSA silent on change of control. vendor-agent · high conf VEND-01 VEND-02

YELLOW Two engineers own the billing/entitlements core; contractor IP assignment unevidenced. eng-agent · high conf ENG-ORG ENG-IP

YELLOW Test coverage materially below the cited figure (~28% vs. ~40% on core services). eng-agent · high conf ENG-CI-01

YELLOW Incident MTTR trending up (~35% over 12 months); on-call concentrated on one squad. sre-agent · med conf OPS-INC-LOG OPS-ONCALL

GREEN The target's identity stack overlaps the acquirer's — a consolidation synergy, not just a risk. integration-agent · high conf VEND-01 PLAYBOOK

Evidence reviewed

Every evidence item opened by the crew during this run, by reference and title — assembled from the tamper-evident audit log, not self-reported.

REF	DOMAIN	EVIDENCE	READ BY
VDR-01	architecture	ARCH-DIAG-01 · platform-topology.pdf ↗	arch-agent
VDR-02	operations	OPS-INC-LOG · incident-log-12mo.csv ↗	sre-agent
VDR-03	security	SEC-CERT-STATUS · soc2-iso-status.pdf ↗	security-agent
VDR-04	security	SEC-PEN-02 · pentest-report-q3.pdf ↗	security-agent
VDR-05	security	SEC-SBOM-01 · sbom-shipped-services.json ↗	security-agent
VDR-06	privacy	PRIV-ROPA · records-of-processing.xlsx ↗	privacy-agent
VDR-07	vendors	VEND-01 · identity-vendor-msa.pdf ↗	vendor-agent
VDR-08	vendors	VEND-02 · payments-msa.pdf ↗	vendor-agent
VDR-09	vendors	VEND-03 · data-enrichment-dpa.pdf ↗	vendor-agent
VDR-10	engineering	ENG-ORG · org-and-oncall.pdf ↗	eng-agent
VDR-11	engineering	ENG-IP · contractor-agreements.zip ↗	eng-agent
VDR-12	engineering	ENG-CI-01 · ci-coverage-artifacts.xml ↗	eng-agent
VDR-13	operations	OPS-ONCALL · oncall-rota.pdf ↗	sre-agent
VDR-14	integration	PLAYBOOK · acquirer-integration-playbook.pdf ↗	integration-agent
VDR-15	architecture	ARCH-COST-01 · cloud-cost-export.csv ↗	cost-agent
VDR-16	security	SEC-QNR · security-questionnaire.pdf ↗	security-agent